

# Notes on human factors problems in process plant reliability and safety prediction

**Taylor, J.R.; Rasmussen, Jens**

*Publication date:*
1976

*Document Version*
Publisher's PDF, also known as Version of record

A. E. K. Risø

Risø - M - 1894

Risø - M - 1894

Title and author(s)

Notes on Human Factors Problems in Process Plant Reliability and Safety Prediction

by

J. Rasmussen
J.R. Taylor

Date September 1976

Department or group
Electronics

Group's own registration number(s)
R-8-76

pages + tables + illustrations

Abstract

The basis for plant operator reliability evaluation is described. Principles for plant design, necessary to permit reliability evaluation are outlined. Five approaches to the plant operator reliability problem are described. Case stories, illustrating operator reliability problems, are given.

Copies to

Available on request from the Library of the Danish Atomic Energy Commission (Atomenergikommissionens Bibliotek), Risø, DK-4000 Roskilde, Denmark
Telephone: (03) 35 51 01, ext. 334, telex: 43116

Fi 25-204

ISBN 87-550-0422 9

CONTENTS

# 1. SOME HUMAN FACTORS PROBLEMS IN PROCESS PLANT SAFETY AND RELIABILITY ANALYSIS

## Introduction

Methods for systematic reliability and safety analysis are gaining increasing acceptance as important tools for industrial process plant design. The size of modern plant units implies high risk potential, and the rapid development of new processes and equipment makes it increasingly difficult to ensure the fulfilment of severe safety requirements by means of specific technical norms and standards.

There is a trend towards the situation when a plant concept will only be acceptable, if it can be demonstrated by a systematic analysis that the safety and reliability requirements will be met by the operating plant. To be susceptible to systematic analysis, a plant design is subject to several constraints related to the limitations and assumptions of the accepted methods of analysis.

Guidelines for system design can therefore be derived by an analysis of the assumptions and limitations underlying the methods for reliability and safety analysis.

The scope of the present note is to discuss the possibility of obtaining guides to man-machine interface design in this way.

The terms, safety and reliability, are not too well defined. In the following discussion, they are used to characterize two different aspects of the sensitivity to accidental maloperation of a process plant.

Reliability is a measure of the ability of a system to maintain the specified function. Classical reliability analysis leads to figures describing the probability that a system will perform the specified function during a given period or at a given time (M.T.B.F., Availability etc.). Reliability analysis is related to the effects caused by absence of specified function. In case of a process plant reliability, figures are used to judge the expected average loss of production; in case of a safety system to judge the expected average loss of protection.

System safety is a measure of the risk or the expected average losses, caused directly by the presence of a state of accidental maloperation, in terms of human injuries, loss of equipment etc. To judge the safety of a system, it is, therefore, necessary to study the probability of specific courses of events initiated by the primary fault, and to relate the probability to the effects of the maloperation, i.e., judgement of system safety is based upon an extensive accident analysis.

In the following discussion a very clear-cut distinction between the methods used for reliability and safety analyses is drawn, and very simplistic descriptions of the methods are used. This is tolerable since the purpose of the discussion only is to reach some preliminary and general conclusions.

## 2. HUMAN FACTORS PROBLEMS IN RELIABILITY ANALYSIS

The definition of the reliability of a system or system component is generally stated in terms of the probability of specified function versus time, such as: "Reliability is defined as that characteristic of an item expressed by the probability that it will perform its required function in the desired manner under all relevant conditions and on the occasion or during the time intervals when it is required so to perform" (Green and Bourne 1972).

Reliability analysis evaluates the possible modes, and probability of, departures from specified function, which is generally rather stable during plant operation of the technical equipment, and unambiguously related to the functional design intention. The human elements of a system, however, cause difficulties in this basic aspect of reliability analysis. Man is an adaptive and learning system element, and may very probably respecify a function or a task. Consider for example a monitoring task from a power plant. The specified task: "If the frequency meter indicates below 58 C/S, disconnect load to save the generator". If an operator has only met readings below 58 C/S due to poor meter performance, he may very reasonably respecify his task: "If ....., then calibrate meter" - and lose a generator (as happened at one stage in the US power black out in 1965). Unless such respecifications are known, reliability prediction will be systematically wrong.

Furthermore, a human operator is a multipurpose element. He may be occupied by another task, and omission of specified function may be due to other events in the system rather than human failure mechanisms.

The method of reliability analysis is to break-down a complex system into parts or components, to a level at which component properties are recognized from widespread use, so that empirical fault data can be collected.

In principle, this break-down must be carried through to a level where component function is invariate with application. This is possible for many standard components, which are designed for a specific function and used according to specifications in system design, e.g., resistors, pumps. In some cases, however, alternative "specified functions" are possible at the level of break-down at which data collection can be arranged.

in practice, e.g., relays and valves can serve to close or break a circuit. Fault data must then be classified according to the function performed, as the related probabilities of failure may be very different for different functions.

In the methods of human reliability prediction in practical use (Meister 1972, Swain 1973), this technique has been transferred to human performance. The complex and often very system-specific human functions are broken down into typical, recurrent, and elementary functions for which reliability data can be collected. Such elementary functions are in practice only distinguishable by their external effects, and are therefore generally characterized as "subtasks".

This technique, however, must be used with extreme caution. Man is in many respects a holistic data processor responding to total situations rather than to individual events or system states. Complex functions may be performed by skilled operators as one integrated and automated response. In this case fault data can only be obtained by a realistic simulation of the total function (Regulinski 1969). Break-down of complex functions is only acceptable if the performance is paced by the system, i.e., cues from the system serve to initiate elementary skilled subroutines individually and to control their sequence. This is the case in many manual tasks, e.g., mechanical assembly tasks, but can probably also be arranged by more complex mental tasks by properly designed interface systems.

The failure properties of a specific function depend upon the operating conditions, and for technical components weighting functions are generally used to modify fault data according to load and environmental effects. The great variability of human performance makes a similar weighting of fault data by "performance shaping factors" mandatory (Swain 1973), but the application is difficult as "operating conditions", such as motivation, stress, fatigue, etc., are badly defined and difficult to quantify; "expert judgements" are generally the only method available.

New problems arise if several internal mechanisms with very different failure probabilities can serve the same external component function. The more flexible a component is, the more difficult will these problems be, especially if the internal organization has autonomous features such as optimization, adaptation, learning.

These are the prominent features of the human elements in a system. The internal function used to perform a specific external task by a man depends strongly upon his training and skill, his prior experiences of system behaviour, his subjective performance criteria etc. Failure data collected from a system in which an operator meets a specific task frequently, and performs it by a sensory-motor response based on a one-step direct association, will have no relation to the failure probability in a system where the demand for the task is infrequent, e.g., as part of an emergency action. The response must then be performed by a sequence of cognitive functions. The resulting problem can only be solved by classifying fault data according to the internal functions used to perform a task. In this situation, weighting of fault data collected from standard, frequently initiated tasks, by means of "performance shaping factors" is not acceptable.

At present, this means that human reliability prediction is only feasible, if "specified function" of human operators is synonymous with a familiar task performed by a skill maintained through frequent use or exercise.

The degree of sophistication of the probabilistic system models used to derive reliability figures characterizing the total system depend upon the quality of the component fault data available. If only bulk data on component failure rates are available, as is typically the case for process plant components, simple probabilistic models are used which represent system structure only as far as to specify whether components functionally are connected in series or parallel during specified system function (reliability block diagrams). If more detailed descriptions of failure mechanisms are available, and if good data are available for failure and repair rates, then much more complete failure modelling becomes worthwhile.

## 3. HUMAN FACTORS PROBLEMS IN SAFETY ANALYSIS

System safety is a measure of the risk - the expected average loss - related to direct effects of the transitions from specified function into a state of accidental maloperation, in terms of human injuries or damage to equipment or environment.

System safety has to be judged from an extensive accident analysis. To identify the course of events following the initiating fault, and to determine the ultimate effect, and its probability, it is necessary to use a detailed functional description of the system including functional properties both within and outside the normal operating régimes of the plant. Different systematic techniques have been developed for this purpose, based on fault tree analysis (Barlow and Lambert 1974) and cause-consequence analysis (Nielsen 1971).

To evaluate the effects of accidental maloperation, statistical data differentiating the different modes of failure of the components must be available. Furthermore, severe effects generally are results of courses of events of extremely low probability, and may be related to component modes of failure which are an a priori improbable and insignificant contributor to component bulk data.

In the analysis of accidents, the human element is the imp of the system. His inventiveness makes it impossible to predict the effects of his actions when he makes errors, and it is impossible to predict his reaction in a sequence of accidental events, as he very probably misinterprets an unfamiliar situation. Some illustrating case stories are found in the appendix.

In practice, human variability makes a quantitative safety analysis unrealistic, unless the system design satisfies a number of conditions.

Like other problems in system design caused by component performance variability, the problems in accident analysis can be circumvented if feed-back functions are introduced, i.e., if feed-back links are introduced in accidental courses of events by means of monitoring and protection functions.

Major losses or human injuries caused by accidental maloperation are typically related to uncontrolled release of stored energy in the system. Apart from accidents caused by spontaneous fractures of energy barriers and explosions, accidents are typically the effects of disturbances of mass or energy balances. There is, therefore, a time delay between the primary cause and the release due to the integrating effect of a disturbed balance. This time delay makes correcting actions possible.

Furthermore, critical variables related to the energy level of the balance can be found which can indicate potentially risky maloperation irrespectively of the preceeding course of events. If a safe state of the system can be defined, and it can be reached through the action of a monitoring and protection function which does not in itself introduce potential risks, an upper bound of the probability of a large class of event sequences leading to the effect which is monitored can be found by a reliability analysis of the protecting function. Such protective functions can be performed by human operators if the task is designed so as to be accessible to human operator reliability analysis, or can be performed by automatic safety systems.

A properly designed protective function enables the derivation of the probability figures needed in accident analysis by means of a reliability analysis of the protective function. The analysis leads directly to upper bounds on probability of courses of events leading to the monitored effect.

It is the extensive use of automatic, protective systems in nuclear power plants that has made it possible to perform a quantitative analysis - including human performance - of the safety level of such installations (Norman Rasmussen et al. 1975).

## 4. CONCLUSION

In principle, a process plant design, which is not based on extensive experience from similar concepts, is only acceptable if performance design targets can be verified by systematic analysis including a quantitative reliability and safety analysis.

A quantitative safety analysis is only possible if the plant design is performed according to guidelines derived from the limitations of the available methods.

The design must be based upon a qualitative accident analysis. Accident potentials cannot be identified by an evaluation of the effects of all possible courses of accidental events. They must be identified directly by a systematic search. Heuristic search strategies related to energy and poisonous matter concentrations have been developed to serve this purpose (Johnson 1973, Powers 1973).

When accident potentials are identified in this way, the sequences of accidental events, which are capable of triggering an accident, must be identified by a systematic, qualitative cause-consequence or fault tree analysis. If a quantitative probabilistic evaluation of the sequences so identified indicates unacceptable risk - or if a quantitative analysis is not possible due to lack of statistical data, monitoring and protection functions must be introduced in the design.

Such functions must be designed so as to be accessible to a quantitative reliability analysis. During the reliability analysis of complex protective systems, it is generally important to keep track of the temporal relations of events, and simple reliability block diagram analysis must be replaced by more sophisticated methods, such as Markov models, renewal theory etc., compatible with a cause-consequence analysis (Nielsen et al. 1974, Taylor 1974, Nielsen et al. 1975).

A protective function can be performed by an automatic system or a human operator.

Reliability analysis of human performance is only feasible if the tasks are performed by sequences of skilled subroutines which are separated and initiated by proper cues from the system. The reliability of more complex and freerunning tasks cannot be predicted directly;

an acceptable prediction of results can only be made in this situation if the effects of the actions are reversible and subject to verification by an operator, following a predictable check procedure.

Automation in this way does not remove man from a system, neither does it force him into the role of a trained robot. Automation serves to replace unexpected tasks at unpredictable moments by tasks which can be planned and trained and which can be based upon qualified decisions, such as supervision, test, and maintenance.

A proper design policy will decrease the influence of unpredictable performance shaping factors, such as stress and motivation. When introducing automatic safety systems, the designer takes responsibility of plant safety and thus relieves the operator from stress. The actions of safety systems are related to rather general criteria concerning the initiating plant states and complex, safe protective systems will decrease plant reliability. The operator thus has a supervisory task to protect the plant from unnecessary automatic safety actions. The responsibility of the operators is related to the reliability of plant operation.

The motivation of plant operators can be maintained in automatic systems if they are allowed to use their abilities and take responsibility in the tasks they are allocated. There is no reason not to permit this as long as the system is designed in a way which allows them to verify the effects of their decisions and actions in a predictable way.

In a period when rapid development of display equipment takes place, and schemes for human error data collection are being planned, there is a need for research in human behaviour in operating industrial plants.

The scope of such research will be to identify and characterize the different data processing functions and strategies used by human operators in real life tasks. The ultimate goal will be to develop guidelines for the design of interface systems which will be used by operators in a predictable way, and to define the attributes of the different categories of operator tasks which should be used when collecting human error data from industrial plants.

## 5. EVALUATING OPERATOR RELIABILITY - ERROR MECHANISMS AND DESIGN PROBLEMS

"ELEMENTARY ACTION MODEL OF HUMAN ERROR

There are several models at present in use for predicting operator reliability during process instrumentation design. Three of them can be described here as examples (from Meister 1971).

1) The AIR Data Store (Payne and Altman 1962) gives times and reliabilities for different operator actions using a Stimulus-Response scheme. By describing the individual steps of a task the time and reliability for the task can be evaluated. Many parameters such as instrument size and placing serve to modify the reliability and timing values.

2) THERP (Swain 1973) is a collection of methods for predicting operator reliability in control and production processes, by dividing tasks into subtasks, at a level for which data can be provided from the THERP data base. An event tree is drawn for the complete operator task, and probabilities are attached to the various event forks. Probabilities for each path from the base of the event tree (correct operation and various error paths) are calculated. The possibility for error correction is treated, and event/operation sequences to deal with the possibility of error recovery are included. Point estimates of reliability for each of the elementary operations, are used, with a standard set of performance shaping factors modifying these. The performance shaping factors are applied as considered appropriate by the behavioural scientist using the technique.

A strong point in the THERP technique is to distinguish clearly between cue, action, and confirmation (feedback). The probability for error is the probability of erroneous cueing or action, multiplied by the probability of misidentifying the confirmation of correct action.

3) Askren and Regulinski's model (1969) has been developed primarily for continuous tasks and aims at finding error rates as a function of time. Laboratory experimental data are used. Time dependent error rates are used, and in this way account for some of the variation treated by performance shaping factors in THERP.

All of these techniques (and also most of the others of which we know) suffer from problems when applied to the situation of safety analysis, for a process operator, in a control room.

Firstly, the breakdown into subtasks is completely oriented towards simple standard sequences of operations on equipment. The subtasks or elementary operations are related to the lowest level of man machine interface action. The subtasks are an interface component engineers view of the human being. For example, in an Aeronutronics report from 1969:

"The conception of operator simulation formed early in the study program was based on several fundamental assumptions in order to develop a suitable working model. The first is that a task can be analysed as a sequence of subtasks, the performance of which has been determined or estimated closely."

PROBLEMS WITH ELEMENTARY ACTION APPROACH - ERRORS IN DECISION MAKING

It is far from clear that this splitting into subtasks is the correct approach when studying trained operators. They tend to regard a complete sequence of such low level subtasks, or elementary operations, as a subtask in itself. Such sequences may be highly trained and often very reliable; generally more reliable than if the operators were to carry out the same operations as an unconnected procedure. In this situation, if errors are made, they are made at a higher level, in deciding to use a procedure in the first place.

Even where a sequence of elementary operations is not highly trained, in many situations errors will arise in decision making, not in carrying out elementary operations.

(There are three cases; a written procedure is available which can be read; a procedure has been learned, which can be remembered; a new procedure must be devised. This last is very common in failure recovery situations).

The effect of this problem on reliability estimates is described below.

A second problem is that the reliability models give the probability of carrying out a task correctly, but do not give the probability for, nor even describe, the other, high risk operations which are carried out instead. Developments in methodology are required to treat this problem.

If tasks, or elementary operations, are classified at too fine a level, not at the level at which errors are made, then it will appear that there is a very large spread in error rates. This can be accounted for formally by using a probability distribution to describe the error rates (Rasmussen et al 1975), but data will be difficult to obtain, and error rate distributions will look very strange - multipeaked if a few reasonably homogenous classes of tasks are used to estimate

A further problem is that of common mode failures at the elementary operation level, arising from decision errors at a higher level. (A common mode failure is a case in which several failure events occur with some causal coupling, so that the events are not statistically independent. For example, for two events A and B, $P(A,B) > P(A).P(B)$. The THERP technique can account formally for some kinds of common mode error (those where similar elementary operations in a sequence are involved), but not all. The presence of a common mode error potential can often alter probabilities for high consequence events by several orders of magnitude.

"SCOPE FOR ERROR' APPROACH

An extension of the mechanistic, man machine interface component approach, can help to solve some of these problems (Taylor 1976). It is assumed that an operator may make an error which results in:

1) Making a single erroneous elementary operation at any time (e.g. pressing a button).

2) In any procedure, omitting an elementary operation.

3) Interchanging the sequence of two elementary operations, or two related operation subsequences.

4) In any procedure, confusing the object of two operations, (e.g. mistaking button A for button B).

5) At any point in a procedure, taking up a section of another procedure (e.g. half way through shut down, commencing a start up).

The consequences of these possibilities can be evaluated, using cause consequence analysis (Nielsen 1974) and those which indicate a high risk can be studied in detail. There is an assumption in the method, that the operator's possibilities for interaction with the plant are limited (to button pushing, knob turning).

By concentrating on <u>risk</u>, rather than probability the number of error sequences to be studied can be limited. (It has been noted that many serious incidents involve <u>sequences</u> of failure or error events, see e.g. Taylor 1973, Johnson 1973). For design purposes, the procedure described can illustrate potential risks, and allow protective instrumentation to be designed.

But the procedure does not approach the problem of determining reliability, in the case of decision making or plant state identification errors. And it does not approach the problems arising when an operator must devise his own procedures.

"LIMITED OPERATOR RESPONSIBILITY" APPROACH

It is possible for a designer to chose a philosophy which minimizes the operator's scope for erroneous decision making ("limited operator responsibility"). If a safety system is provided which can return a plant to a safe state from any unsafe state ("designed safety actions"), then the operator has no freedom to introduce risk. (He still has freedom to optimize production). If the operator is nevertheless required to carry out some "required operator safety actions", (see ANSI draft standard N660), then procedures can be given for these, and training, so that the operator has no decisions to make, and reliability analysis becomes simpler (see table 1). Not all systems can be designed using this philosophy however. It requires that all failure states have been foreseen by the designer, including those arising from operator and design errors! Or at least, the designer must be prepared to take responsibility for all failure states, and all "unplanned operator actions".

If a designer is prepared to accept responsibility for plant safety, and to carry out the necessary thorough analysis, then an alternative to operator error probability calculation presents itself. That is, to design an interlock system which prevents the operator errors. Systematic techniques for design of such interlock systems have been described (Rudd, Taylor). If such an interlock system is constructed, then the problem of safety in the face of foreseeable operator errors becomes one of interlock system reliability.

If a correspondingly thorough analysis is carried through for risks arising from other plant disturbances, not operator errors, then the operator's function becomes largely one of controlling the plant to control these disturbances to maintain a safe operating state and prevent shutdown. For this purpose reliability analysis procedures, rather than risk analysis, are acceptable. However, such thorough safety system design is at present expensive, in terms of engineer effort, for the majority of process systems.

An approach which deals directly with the risks involved in decision making and erroneous use of procedures, is to study complete case stories from actual accidents, and classify them. It seems possible, from cases we have looked at, to find definite error phenomena connected with the way operators think about a process plant.

| Everyday Operating Procedure | Safety Procedure |
|---|---|
| May be very free, but requires feed back in order that OP can confirm his own decisions. | Must be highly trained in order that reliability data can be collected and reliability evaluation is valid. |
| To allow freedom in everyday operating procedures, requires a very thorough and reliable automatic safety system, and/or very highly trained safety procedures. | Requires cueing in order that reliability data can be collected and reliability evaluation is valid. |
| Intended to optimize production and protect system from unnecessary safety shutdown. | Intended to protect against accidents. |

Table 1: Limited operator responsibility approach.

This approach is similar to that described by Russel Davis (1958). He describes three error phenomena:

False hypothesis

People respond to situations as they conceive them to be, not as they are.

Preoccupation

By concentrating on one part of a problem, a more important aspect is overlooked.

Emergency mechanisms

In an untoward incident, a person reacts in a way which his previous experience has taught him is likely to be effective, even in inappropriate situations.

We have found a need for more detailed classes.

Reinterpretation as instrument error

When a very improbable accident indication is given, the operator reinterprets this as instrument error. He evaluates his action on the basis of probability, not on risk. (He may recalibrate instruments rather than take readings at face value).

Similar situation switchover

When the cues provided by the plant in one state are the same as those for another state, in another procedure, the operator may switch procedures (presumably after some distraction).

Evaluation on the basis of partial information

It is well known that operators habitually base their decisions on readings from just part of the plant information, ignoring some of the information displayed. This can cause a mismatch between the operator's performance and the instrumentation engineer's or reliability analyst's expectations.

Misidentification of equipment

Closely located, similar equipments are confused.

Inter operator communication error

Operators seldom work completely alone, they communicate with each other. If an indication of plant state is communicated incorrectly, then an accident may result.

Private procedures

Operators may develop their own, unsafe, procedures, because they are more convenient.

Examples of incidents involving these kinds of phenomena are given in the appendix. Unreliability from these mechanisms should be regarded as supplementary to the basic elementary operation random errors.

While an approach involving the collection of case-data concerning different decision making errors would be interesting, it would suffer from the same kinds of criticism as the "elementary operation" approach. It would indicate only some of the performance shaping factors required. It would tend to mix data, classifying errors due to different mechanisms together (with consequent probability estimation errors, especially for "two peaked" error probability distributions). And it would lead to many causes of common mode failure being overlooked.

OPERATOR MODEL APPROACH

The classification of case stories should rather be taken to indicate that a deeper theory of operator behaviour and decision making should be possible. If a model of the process operator can be produced which describes how he makes decisions, and carries out tasks, how he observes and responds to cues, then more detailed and more firmly based estimates of error probability can be made. Also the various factors which determine probability can be evaluated more accurately. In some cases, it should be possible by a deterministic analysis to detect the possibility of high risk situations - for example when one of the operators possible decision making routines overlooks unlikely but dangerous plant states. In order to come further in treating plants for which perfect safety systems are impossible, such an approach is necessary.

The patterns that emerge in some of the case stories given in the appendix suggest that such a program of work (fig. 1) could well meet with success. Some steps in this direction have already been taken at Risø (Rasmussen 1969, 1973, 1974, 1976). But further, there is a large body of research on operator ergonomics, and on decision making, which by adopting the operator model approach can be made directly relevant in risk analysis and safety system design.

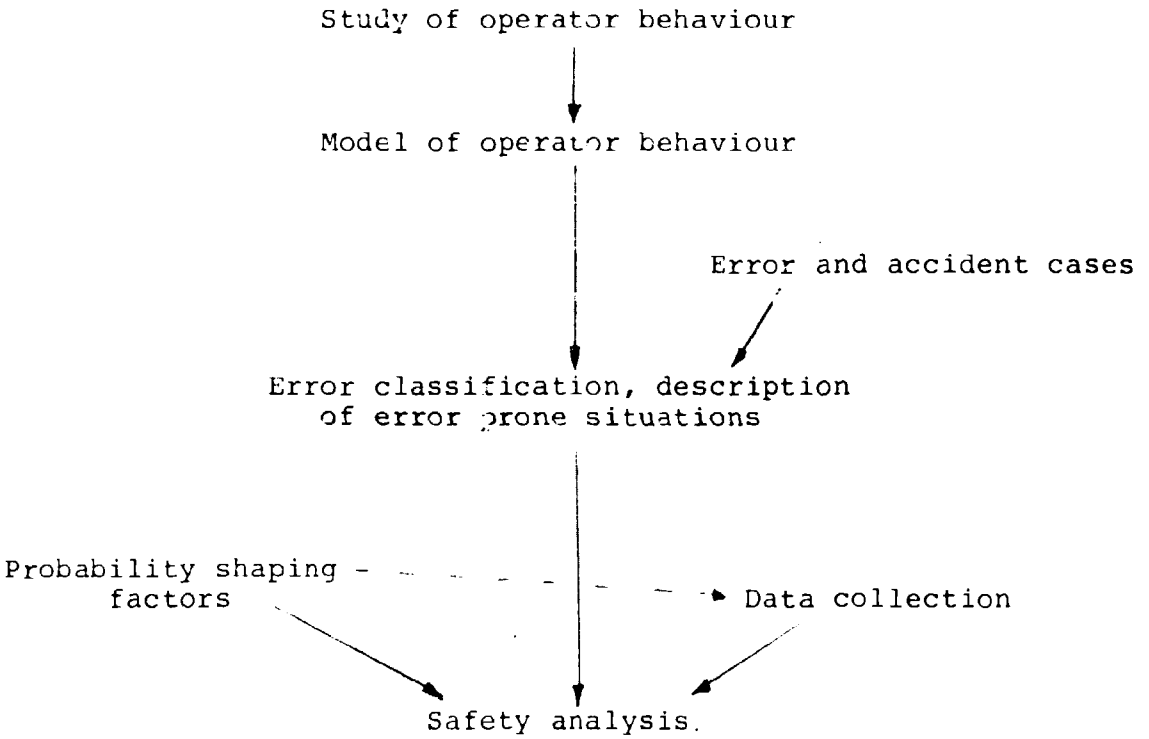


Fig. 1 Steps toward a detailed analysis of operator error.

# APPENDIX

## CASE STORIES

The following case stories illustrate some of the phenomena which make reliability and safety prediction difficult. Unless otherwise indicated, they have been obtained from private communications with process plant operators. In some cases, details have been deleted, to protect both the innocent, and the unlucky.

Case:

During normal operation of a process plant the power supply to the instrumentation and the control console slowly disappears.

Investigation:

The manual main circuit breaker in the flywheel motor-generator supply is found to be in the off position. The conclusion of an investigation was that a roving operator, checking cooling towers and pumps, inadvertently had switched from a routine check round to the friday afternoon shut down check round and turned off the supply. The routes of the two check rounds are the same, except that he is supposed to pass by the door of the generator room on the routine check, but to enter and turn off the supply on the shut down check. Something "en route" obviously has conditioned him for shut down check (sunshine and day dreams?). The operator was not aware of his action, but did not reject the condition.

Comments:

Human operators move around in the plant, and it can be difficult to predict where in the causal structure of the plant he interferes. His actions may not be initiated by an event in the system or specified by a program, but by subconscious mechanisms, i.e. it is difficult to predict when he interferes and how.

Case:

During start up of a process plant the plant is automatically shut down during manual adjustment of a cooling system.

Investigation:

During start up the operator monitored the temperature of the primary cooling system and controlled it by switching off and on the secondary cooling pumps to avoid water condensation in the primary system due to the cold cooling water. On this occasion he observed the temperature to reach below the low limit, signalling a demand to switch off the secondary pumps, while he was talking to cooperator over the phone. He then switched off the primary pumps and the plant immediately shut down automatically. He did not recognize the cause immediately, but had to diagnose the situation from the warning signals.

The control keys for the two sets of pumps are positioned far apart on the console. A special routine exists during which the operator switches the primary pumps on and off to allow an operator in the basement to adjust pump valves after pump overhaul while they communicate by phone. Is the cause of the event subconscious switching of procedures due to the phone call?

Comment:

The case illustrates some features of operator behaviour:

- Change in procedures by secondary unpredictable events or conditions.

- The operator introduces couplings in the system by coincident omission of one task and performance of an inappropriate action.

- The risk may be related to the inappropriate and unpredictable act rather than to the omission.

Case:

An experimental plant shuts down automatically during normal operation due to inadvertent manual operation of cooling system shut off valve.

Investigation:

A safety shut off valve in the cooling system which is routinely closed during post shut down check procedures was closed manually. The valve control switch is placed behind the operating console, and so is the switch of a flood lightning system used for special operations monitored through closed circuit television. The switches are neither similar not closely positioned. The operator has to pass the valve switch on his way to the flood light switch.

In this case the operator went behind the console to switch off the flood light, but operated the shut off valves which caused plant shut down through the interlock system.

Comments:

Strongly automated and stereotyped action sequences are frequently initiated by a single conscious decision. If the action takes some time, e.g., you have to move to another place to perform the action, the mind may return to other matters, and the sequence is vulnerable to unpredictable conditions, particularly if the sequence intended in some of the steps overlap other familiar and automated sequences.

Case:

Butadiene explosion at Texas City.
Plant Safety and Loss Prevention. Volume 5, CEP.

Investigation:

"Loss of butadiene from the system through the leaking overhead line motor valve resulted in substantial changes in tray composition ...".
..."The loss of liquid in the base of the column uncovered the calandria tubes, allowing the tube wall temperature to approach the temperature of the heat supply. The increased vinylacetylene concentration and high tube wall temperature set the stage for the explosion which followed".
..."The make flow meter showed a continuous flow; however, the operator assumed that the meter was off calibration since the make motor valve was closed and the tracing on the chart was a straight line near the base of the chart. The column base level indicator showed a low level in the base of the column, but ample kettle vapor was being generated".

Comment:

Wisdom after the event tells that closed valve together with continuous flow signals possible leak, and the risk implied calls for investigation. The skilled operator, however, conforms his observations individually with his expectations or process feel. If abnormal observation refers to a familiar situation, he sees no problem and does not investigate the matter. You cannot predict his response without knowing his daily experiences. It can be difficult to predict the probability that an operator performs a specified function because he may have respecified his function - sometimes with good reason.

This can happen, even if there is a clear prewarning:

Case:

Melt down of fuel element in nuclear reactor. Nuclear Safety, September 1962.

Investigation:

Certain tests required several hundred process coolant tubes to be blocked by neoprene disks. 7 disks were left in the system after the test, but were located by a test of the gauge system that monitors water pressure on each individual process tube. For some reason the gauge on one tube was overlooked, and it did not appear in a list of abnormal gauge readings prepared during the test. There was an additional opportunity to spot the blocked tube when a later test was performed on the system. This time the pressure for the tube definitely indicated a blocked tube. The shift supervisor failed, however, to recognize this indication of trouble. The gauge was adjusted at that time by an instrument mechanic to give a midscale reading which for that particular tube was false. This adjustment made it virtually certain that the no flow condition would exist until serious damage resulted.

Case:

Docket 50219-167: Two diesel generators set out of service simultaneously.

Event sequence:

8.10 permission to perform surveillance test on containment spray system No. 1 including electrical and mechanical inspection of diesel generator No. 1.

8.20 permission to take diesel No. 2 out of service for oil addition.

Both systems out of service for 45 min. Foreman overlooked test of No. 1 system when permitting diesel No. 2 operation.

Comment:

Coincident unavailability of redundant systems caused by improper timing of routine tasks. Difficult to predict due to dependence on station "software" vulnerable for changes and oversight due to absence of cues from the system supporting attention.

Case:

Docket 50-219-378. Momentary interruption of 125 DC power supplying instrumentation with various safeguard systems.

Investigation:

Electrical ground on 125V distribution bus resulting in electricians being called for trouble shooting and repair. "Electrical grounds of this nature have been an infrequent problem in the past and as of this time no approved procedures have been developed."

The electrician placed a jumber in a wrong position and effectively did not have the buses paralleled as desired.

Comment:

Procedures for repair on live systems cannot be issued for all possible faults. The consequence of possible faults during work on electrical cabling and wiring terminal systems is unpredictable.

General:

Steps in manual sequences, which are not initiated by system cues, but depending solely on procedures, are subject to omission or change of sequence.

- Reclosing test valves Docket 50-133- , 50-219-193, 50-219/74/21.
- Pressure equalizing before valve operation Docket 50-219-153.
- Inverting sequence of operations Docket 50-219-169.
- Temperature equalizing Docket 50-219-245 removal of test fixtures Docket 50-155-311.

Case:

Overpressurization of reactor coolant system. Docket 50-295-135.

Investigation:

Charging pump started to increase pressure. System pressure increased gradually. Station operator distracted by telephone call and left the area of the pump control switch.

Comment:

Operators are multipurpose components. Faults

in one function can be caused by events related to other functions. Causal couplings are introduced.

Case:

A control computer for a reactor fuel charging machine showed a repeated alarm, but the alarm was ambiguous and unspecific. The operator reset the machine, and continued with an erroneous loading schedule until a fuel melt down occurred.
Nuclear Safety Vol 12 No. 1, Jan. 1971, pp 35-39.

Comment:

Unreliable instrumentation leads to mistrust. If an incident occurs it may be interpreted as instrument failure.

Conclusion:

Instrumentation which is important for safety should be diversely redundant, and the designer should check that the operator is able to and does make use of this redundancy in practice.

Case:

A reactor was in the hot shut down condition, with stream bypassing the turbine to the condenser and bypassing of stream to the condenser. On increasing temperature after clearing the original transient, the main stream control valves suddenly opened, resulting in a major pressure transient, and shut down of the reactor.
Docket 50-133-37.

Cause:

The main control valve signal was gated out by a temperature trip. The procedure for switching to manual control during trip was not followed, and an integral controller signal integrated the measured error in stream flow when compared with set point. When a sufficiently high temperature was reached, the integrated "error" signal was applied to the valve so that it opened fully.

Comment:

1) It is not clear to what extent operators follow procedures, nor to what extent procedures are all practical.
2) It is hard for operators to foresee the workings of instruments - especially in abnormal plant situations.

Case:

Hydrogen explosion due to repair error. Nuclear Safety Vol. 17 No. 2, March 1969, page 249.

" An isolation valve in the off-gas system was found to be closed instead of open. This forced off-gas from the steam jet air ejector through a loop-seal drain line from the 48-in.-diameter holdup line to this sump and back to the dilution fans prior to being discharged up the Elevated Release Point.

The valve was found to be closed even though the control-room valve position indicating lights and the control switch showed the valve to be open. Changes had been made on the electric wiring to this valve during the previous outage. Approval had been given to red-line drawings of the valve and some associated valves that are part of the additional off-gas treatment equipment that will be put in service later this year. But authorization had not been given to change any wiring associated with the valve. Personnel involved in making the wiring change thought they had verified the proper position of the valve by observing the position of the slotted notch at the top of the stem. The butterfly valve gate, however, was not parallel to the slot as they had believed.

An explosive meter was not used to sample the gases flowing from the sump, because no indication of hydrogen had been found in the past when this sump had been opened."

Comment:

The operator's or repair man's information about component performance may be in error. In extreme cases, many components of the same type may be affected by erroneous installation or adjustment resulting from information errors.

Case:

Off gas explosion due to ice build up and instrument interpretation error. Nuclear Safety Vol. 17 No. 4, July 1976, page 493

..."The first indication of a problem came in the early morning hours when the control-room alarm indicated a low flow at the discharge of the off-gas dilution fan. Because of low flow, the instrumentation automatically started the

other fan and the operators then shut down the first one. Previous to the alarm the flow records for the elevated release point of the diluted off-gas had penned a flow decrease from about 1.5 $m^3$/sec (2800 cfm) to about 1 $m^3$/sec (2200 cfm) over a period of several hours. However, no flow increase occurred after the second fan started, and a few minutes later a low-flow alarm sounded once again. The standby off-gas treatment fan was then started, but there was still no increase in flow on the recorder for the elevated release point, and the flow indication from the standby off-gas treatment fan was also low. The shift supervisor and an operator went to the off-gas building to investigate and noticed that the building did not seem to be at its normal negative pressure and that the building air monitor indicated an increase in activity. The two went next to the area of the elevated release point but saw no indication of the problem. They turned to the off-gas building; however, the building air monitor was then reading full scale, so they left immediately. Not too long thereafter the building was destroyed by an explosion".....

..."The incident was apparently caused by an ice plug that formed at the top of 100-m (325 ft) elevated release point pipe."....

..."The flow reduction progressed gradually as the ice built up and went undetected because the observed reduction, as indicated by the instrumentation, was well within normal variations caused by the temperature changes. This flow instrumentation evidently had a history of unreliability. In fact, after the complete loss of flow caused by the explosion, the recorder still indicated a flow of 54 $m^3$/min (2000 cfm)."

Comment:

This is possibly "reinterpretation as instrument error" at a subconscious level!

REFERENCES

Aeronutronics
AD-431 611
Human Factors Aspects of Reliability
Newport Beach, California
January 1964

ANSI draft Standard N660, September 1975
Proposed American National Standard Criteria for Safety Related Operator Actions

Askren, W.B. and Regulinski, T.L. 1969
Mathematical Modelling of Human Performance Reliability

Davis, R. 1958
Human Errors and Transport Accidents

Green, A.E. and Bourne, A.J. 1972
Reliability Technology
Wiley-Interscience
Copyright 1972

Johnson, W.G.
SAN 821-2
MORT
The Management Oversight and Risk Tree
Prepared for the U.S. Atomic Energy Commission
Submitted to AEC
February 12, 1973

Lambert, H.E. and Barlow, R.E.
Introduction to Fault Tree Analysis
March 12, 1975
In "Reliability and Fault Tree Analysis", SIAM 1975

Meister, D. 1971
Comparative Analysis of Human Reliability Models
Human factor dept., Bunker Ramo Corp.
Westlake Village, California
AD-734 432

Nielsen, D.S. 1971
The Cause-Consequence Diagram Method as a Basis for Quantitative Reliability Analysis
Risø-M-1374
ENEA CREST, May 26-28 1971

Nielsen, D.S. 1974
Use of Cause-Consequence Charts in Practical Systems Analysis
Risø Report Risø-M-1743

Nielsen, D.S. and Runge, B. 1974
Unreliability of a Standby System with Repair and Imperfect Switching
IEEE Trans. Rel. R-23 (1974) 17-24

Nielsen, D.S., Platz, O. and Runge, B. 1975
A Cause-Consequence Chart of a Redundant Protection System
IEEE Transactions on Reliability, Vol. R-24, No. 1
April 1975

Payne, D. and Altman, J.W. 1962
An Index of Electronic Equipment Reliability
Report AIR-C-43-1/62-FR

Powers, G.J. and Tomkins, I.C. 1973
Fault Tree Synthesis for Chemical Processes
AICHE Journal Vol. 20 No. 2, page 376-387

Rasmussen, N. et al 1976
Reactor Safety Study, Appendix 2
WASH-1400

J. Rasmussen 1969
Man-Machine Communication in the Light of Accident Records
July 1969
S-1-69
Reprinted from IEEE-GMMS, ERS International Symposium on Man-Machine Systems, Cambridge, 1969

J. Rasmussen 1973
The Role of the Man-Machine Interface in Systems Reliability
November 1973
Risø Report R-10-73
Reprinted from NATO Conference on Generic Techniques in Systems Reliability Assessment. Liverpool, July 1973

J. Rasmussen 1974
The Human Data Processor as a System Component
Bits and Pieces of a Model
June 1974
Risø Report R-8-74

J. Rasmussen 1976
Outlines of a Hybrid Model of the Process Plant Operator
Risø Note N-7-76

Regulinski, T.L. 1973
Human Performance Reliability Modelling in Time Continuous Domain
From NATO Conference on Generic Techniques in Systems Reliability Assessment
Liverpool, July 1973

Rivas, J.R., Rudd, D.F. and Kelly, L.R.
Computer Aided Safety Interlock Systems
AICHE Journal Vol. 20 No. 2
March 1974
pp 311-319

Swain, A.D. 1973
Improving Human Performance in Production
Industrial and Commercial Techniques Ltd.
30-32 Fleet St. London EC4

Taylor, J.R. 1973
Design Errors in Nuclear Power Plants
Risø Report Risø-M-1742

Taylor, J.R. 1974
Sequential Effects in Failure Mode Analysis
Risø Report Risø-M-1740
An edited version is given in Reliability and Fault Tree-Analysis ed. R.E. Barlow, J.B. Fussel, N.D. Singpurwalla, SIAM, 1975

Taylor, J.R. 1976
Interlock Design Using FAult Tree and Cause-Consequence Analysis
To be published